



SPYWOLF

Security Audit Report



Completed on
July 20, 2022

MADE IN USA 

 @SPYWOLFNETWORK

 @SPYWOLFNETWORK

 SPYWOLF.CO



OVERVIEW

This audit has been prepared for **LooBr** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threats	08-A/08-C
Good Practices	09
Tokenomics	10
Team Information	11
Website Analysis	12
Social Media & Online Presence	13
About SPYWOLF	14
Disclaimer	15



LooBr



PROJECT DESCRIPTION

LooBr is a revolutionary all-in-one cross-chain social media integrated NFT marketplace for players, creators, and traders. We offer state-of-the-art and custom-designed social media features for all users.

LooBr is the second product of MetaRuffy International FZCO based in Dubai; the first product was RuffyWorld, our part of the Metaverse, with a focus on the entertainment sector.

Release Date: Relaunch to be held on July 29, 2022

Category: NFT Marketplace / Metaverse



CONTRACT INFO

Token Name

LooBr

Symbol

LooBr

Contract Address

0x2d537cc7a9aA092ca3dD1Ee542c0B73560cB14f0

Network

Binance Smart Chain

Language

Solidity

Deployment Date

July 19, 2022

Verified?

Yes

Total Supply

100,000,000,000

Status

Not launched

TAXES

Buy Tax

10%

Sell Tax

10%

*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(As of July 20, 2022)



Liquidity

Not added yet



Burn

No burnt tokens

Status:
Not Launched!

MaxTxAmount
No limit

DEX:
PancakeSwap

LP Address(es)

Liquidity not added yet

Reward Token:



Meta Ruffy (metaruffy.io)

CA:
0x2456BBAD80BfAD346AecEa45fA38C81a6963132D



TOKEN TRANSFERS STATS

Transfer Count	2
Uniq Senders	2
Uniq Receivers	2
Total Amount	147302500000 LooBr
Median Transfer Amount	99999999999.99998 LooBr
Average Transfer Amount	73651250000 LooBr
First transfer date	2022-07-19
Last transfer date	2022-07-19
Days token transferred	1

SMART CONTRACT STATS

Calls Count	17
External calls	13
Internal calls	4
Transactions count	14
Uniq Callers	5
Days contract called	2
Last transaction time	2022-07-20 04:50:59 UTC
Created	2022-07-19 18:37:56 UTC
Create TX	0xdd6784951dd21a954a9ca42b795fd6ceba0d199286c199569885453f1a214121
Creator	0x79003a1052658f3b664cc080a001875d501be4b1

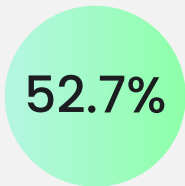


FEATURED WALLETS

Owner address	0x79003a1052658f3b664cc080a001875d501be4b1
Dev fee receiver	0xe272764ac4d42b11af1531c5fc6d48787eb9496b
Marketing fee receiver	0x0ba86aee0d1e6f0a86c26e84754bb7ed83bb280d
LP address	Liquidity not added yet

TOP 3 UNLOCKED WALLETS

1



Same as owner



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

Medium Risk

Owner can set buy/sell/transfer fees up to 20%.
Combined buy+sell=40%.

```
function updateBuyFees(uint256 reward, uint256 marketing,
  uint256 dev, uint256 burn) external onlyOwner {
  buyDividendRewardsFee = reward;
  buyMarketingFee = marketing;
  buyDevFee = dev;
  buyBurnFee = burn;
  buyTotalFees = reward.add(marketing).add(dev).add(burn);
  require(buyTotalFees <= 20, "Total Fee must be less than 25%");
  emit UpdateBuyFees(reward, marketing, dev, dev);
}

function updateSellFees(uint256 reward, uint256 marketing,
  uint256 dev, uint256 burn) external onlyOwner {
  sellDividendRewardsFee = reward;
  sellMarketingFee = marketing;
  sellDevFee = dev;
  sellBurnFee = burn;
  sellTotalFees = reward.add(marketing).add(dev).add(burn);
  require(sellTotalFees <= 20, "Total Fee must be less than 25%");
  emit UpdateSellFees(reward, marketing, dev, burn);
}

function updateTransferFee(uint256 _transferfee) external onlyOwner {
  transferFee = _transferfee;
  require(_transferfee <= 20, "transfer fee limit");
  emit UpdateTransferFee(_transferfee);
}
```

- Recommendation:
 - Considered as good tax deduction practice is buy and sell fees combined no to exceed 25%



FOUND THREATS

Low Risk

Owner can exclude address from fees.

```
function setIsFeeExempt(address holder, bool exempt) external onlyOwner {  
    isFeeExempt[holder] = exempt;  
    emit SetFeeExempt(holder, exempt);  
}
```

Owner can withdraw native chain tokens from the contract (BNB).

```
function clearStuckBalance(uint256 amountPercentage) external onlyOwner {  
    uint256 amountBNB = address(this).balance;  
    payable(msg.sender).transfer((amountBNB * amountPercentage) / 100);  
    emit ClearStuckBalance(amountPercentage);  
}
```

Owner can withdraw reward tokens from dividend distributor.

```
function purgeBeforeSwitch() external onlyOwner {  
    dividendDistributor.purge(msg.sender);  
}  
  
function purge(address receiver) external override onlyToken {  
    uint256 balance = REWARD.balanceOf(address(this));  
    REWARD.transfer(receiver, balance);  
}
```



FOUND THREATS

Informational

PinkAntiBot implementation line is missing in the constructor.

```
pinkAntiBot.setTokenOwner(msg.sender);
```

*For more information about PinkAntiBot implementation, visit their github page:
<https://github.com/pinkmoonfinance/pink-antibot-guide>



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

LooBr

GOOD PRACTICES FOUND

- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot set a transaction limit
- ✓ The smart contract utilizes "SafeMath" to prevent overflows

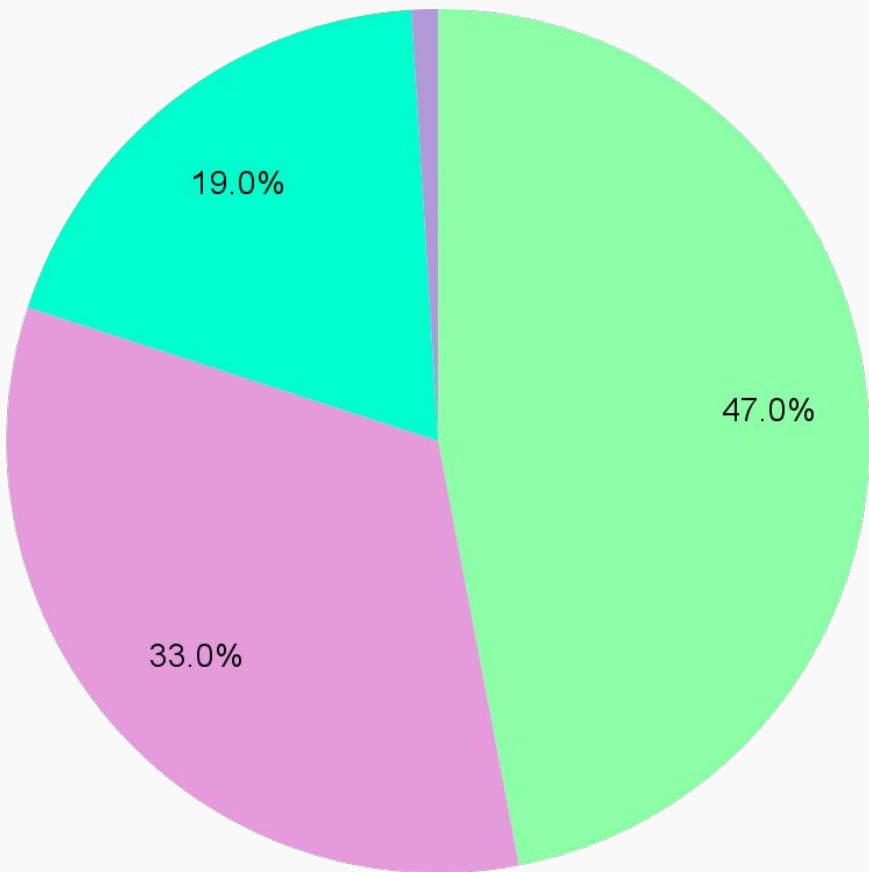


*The following tokenomics are based on the project's whitepaper:

Total Supply: 100,000,000,000

- 47% Presale: 47,302,500,000
- 33% Burn: 32,697,500,000
- 19% Ecosystem (Exchange listings): 19,000,000,000
- 1% Team tokens: 1,000,000,000

- 47% Presale
- 33% Burn
- 19% Ecosystem
- 1% Team tokens



TOKENOMICS



THE TEAM

✓ The team at LooBr is publicly doxxed.

They are the same founders of METARUFFY, a well known project that gives users the opportunity to become one of the early birds who Build Entertainment Stadiums, Resorts, Pub's, Social-Gaming, Sport's, Dating and NFT on the METAVERSE.



CIHAN
CEO, FOUNDER



FOX
COO, OPERATING



SAFI
CTO, IT



ANNA MARIA
CCO, CREATIVE



DANIEL
LEAD STRATEGIC ADVISOR



KENPACHI
LEAD BUSINESS DEVELOPMENT &
INNOVATION



AT
GUERILLA CREATIVE DIRECTOR



RAMEEN
LEAD MARKET MAKING



ANDRE
HEAD OF SOCIAL MEDIA



CRYPTOKING
LEAD INVESTMENT DIRECTOR



MOHIT
GUERILLA MARKETING EXPERT



VOLODYMYR
BLOCKCHAIN DEVELOPER



OSMAN
PR EXPERT





WEBSITE

Website URL
<https://loobr.com/>

Domain Registry
<https://www.godaddy.com>

Domain Expiration
Expires on 2024-06-29

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

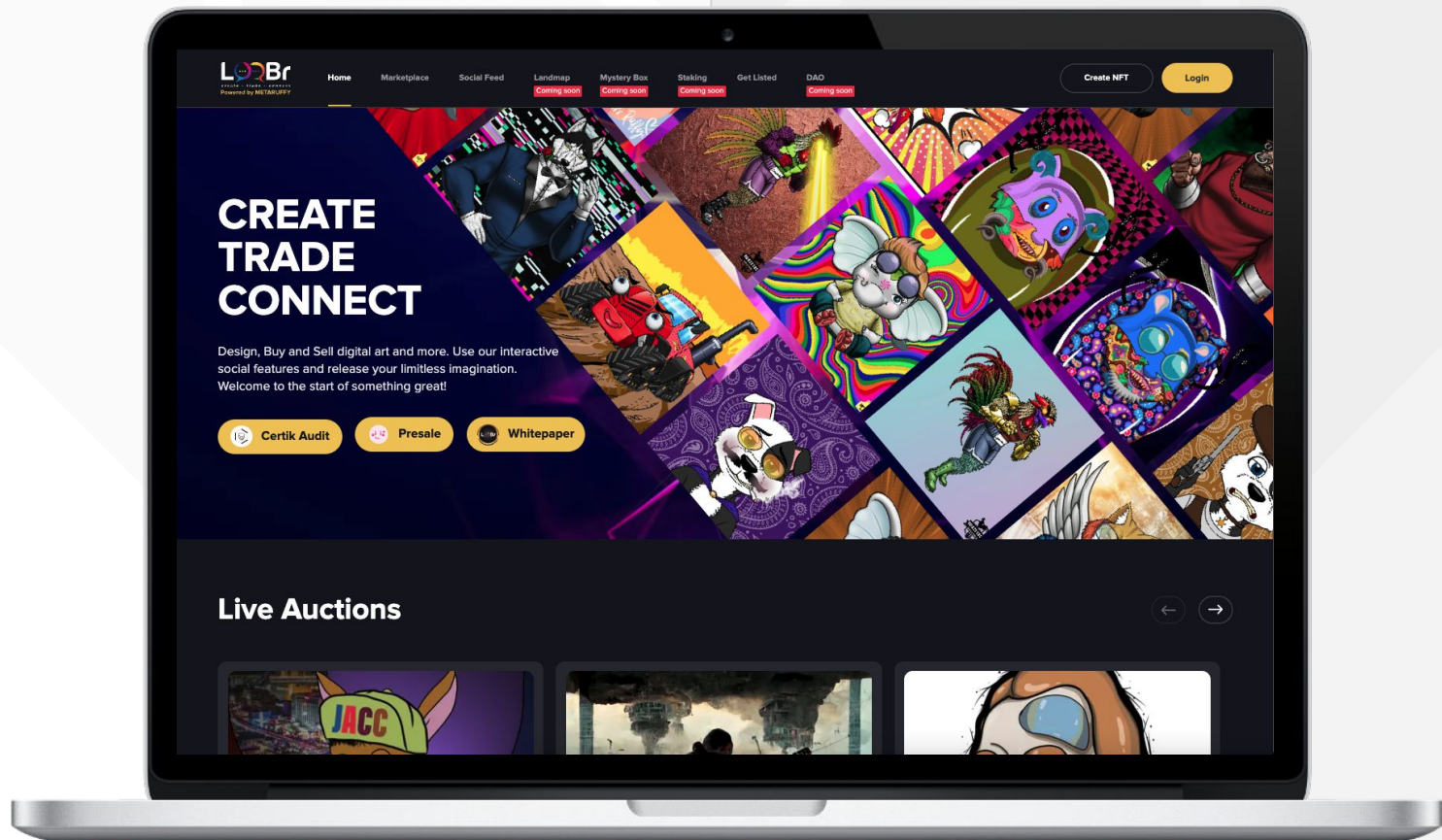
Design
Unique design, very nice
color scheme and graphics.

Content
Informative, no grammar
mistakes.

Whitepaper
Well written, explanatory.

Roadmap
Yes, goals set at 3 phases
without time frames.

Mobile-friendly?
Yes



loobr.com

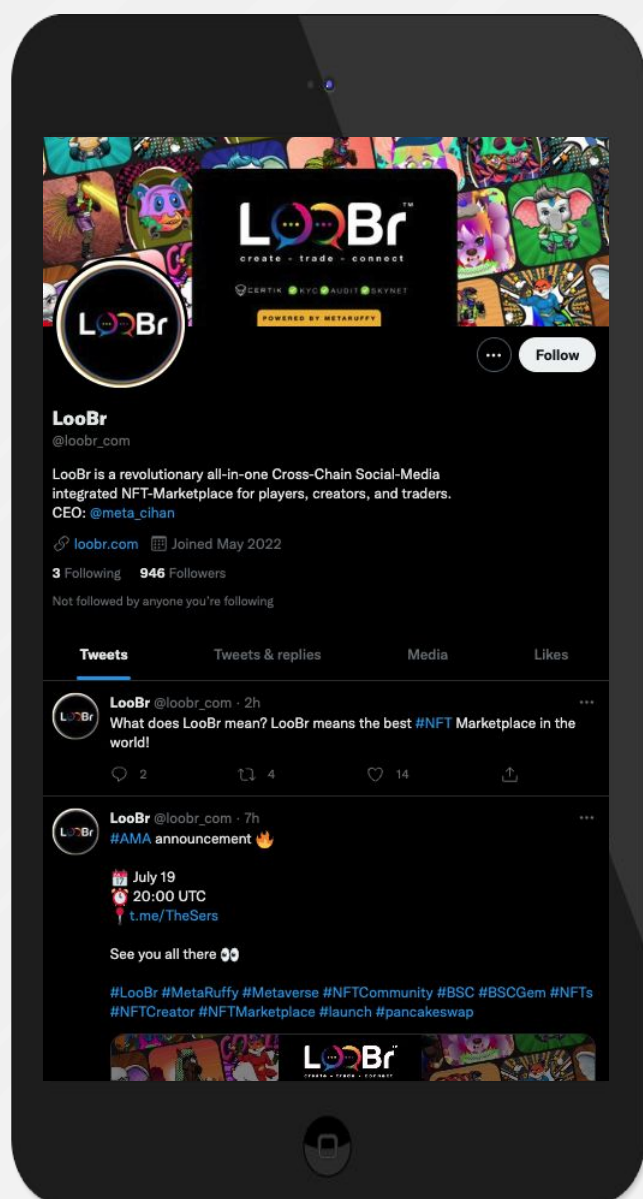


SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

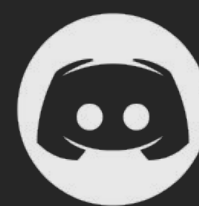
Project's overall social media presence consists of plenty of active members and posts.



Twitter

@loobr_com

- 946 Followers
- Active



Discord

@metaruffy

- 1469 members
- Active



Telegram

@loobr_com

- 3932 members
- Active mods
- Active members



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[SPYWOLF.NETWORK](https://spywolf.network)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFOFFICIAL](https://t.me/SPYWOLFOFFICIAL)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://github.com/SPYWOLFNETWORK)



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.